

AUTHENTICATION DOCUMENT, AUTHENTICATION FORM, AND SYSTEM FOR ISSUING AND VERIFYING AUTHENTICATION DOCUMENT

Publication number: JP2002062803

Publication date: 2002-02-28

Inventor: MORITA YORIKO

Applicant: DAINIPPON PRINTING CO LTD

Classification:

- international: B42D11/00; G06F19/00; G06K19/06; G06Q10/00;
G06Q50/00; G07D7/20; G09C1/00; B42D11/00;
G06F19/00; G06K19/06; G06Q10/00; G06Q50/00;
G07D7/00; G09C1/00; (IPC1-7): G09C1/00; B42D11/00;
G06F17/60; G06F19/00; G06K19/06; G07D7/20

- European:

Application number: JP20000252054 20000823

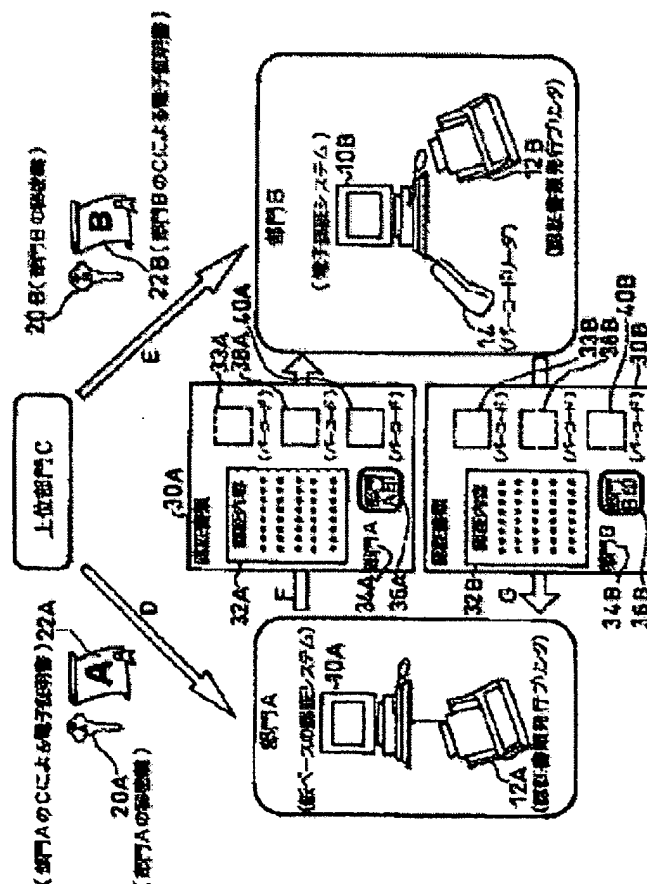
Priority number(s): JP20000252054 20000823

Report a data error here

Abstract of JP2002062803

PROBLEM TO BE SOLVED: To provide an authentication document applicable to both of an electronic authentication system and a paper-base authentication system.

SOLUTION: Visibly confirmable authentication contents 30A, 30B, authenticator information 34A, 34B, and authenticator's seal imprints 36A, 36B are described in authentication certificates 30A, 30B together with bar codes 33A, 33B of authentication contents data in which the authentication contents 32A, 32B are described, bar codes 38A, 38B of electronic signature data enciphering the authentication contents data, and bar codes 40A, 40B of electronic certificate data of the authenticator.



Data supplied from the esp@cenet database - Worldwide

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-62803

(P2002-62803A)

(43) 公開日 平成14年2月28日 (2002.2.28)

(51) Int.Cl. ⁷	識別記号	F I	テームコード (参考)
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 Z 3 E 0 4 1
			6 4 0 B 5 B 0 3 5
B 4 2 D 11/00		B 4 2 D 11/00	U 5 J 1 0 4
G 0 6 F 17/60	1 4 0	G 0 6 F 17/60	1 4 0
19/00	3 0 0	19/00	3 0 0 N

審査請求 未請求 請求項の数21 O L (全 9 頁) 最終頁に続く

(21) 出願番号 特願2000-252054 (P2000-252054)

(22) 出願日 平成12年8月23日 (2000.8.23)

(71) 出願人 000002897

大日本印刷株式会社

東京都新宿区市谷加賀町一丁目1番1号

(72) 発明者 森田 より子

東京都新宿区市谷加賀町一丁目1番1号

大日本印刷株式会社内

(74) 代理人 100080458

弁理士 高矢 諭 (外2名)

Fターム (参考) 3E041 AA10 BA15

5B035 AA15 BB01 BC00

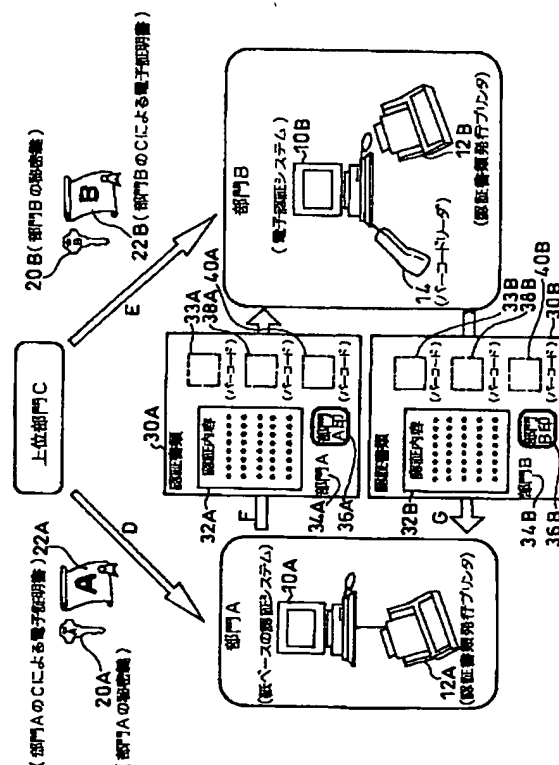
5J104 AA09 LA03 LA06 NA02 PA13

(54) 【発明の名称】 認証書類、認証用紙、及び、認証書類の発行・検証システム

(57) 【要約】

【課題】 電子認証システムと紙ベースの認証システムのどちらでも利用可能な認証書類を提供する。

【解決手段】 認証書類30A、30Bに、視覚により確認可能な認証内容32A、32B、認証者情報34A、34B及び認証者印影36A、36Bと、前記認証内容32A、32Bを記述した認証内容データのバーコード33A、33B、該認証内容データを暗号化した電子署名データのバーコード38A、38B、認証者の電子証明書データのバーコード40A、40Bと共に記載する。



【特許請求の範囲】

【請求項1】視覚により確認可能な認証内容、認証者情報及び認証者印影と、

前記認証内容を記述した認証内容データのバーコード、及び、該認証内容データを暗号化した電子署名データのバーコードと、

が共に記載されていることを特徴とする認証書類。

【請求項2】前記認証書類に、更に、認証機関による認証者の電子証明書データのバーコードが記載されていることを特徴とする、請求項1に記載の認証書類。

【請求項3】前記認証内容データが、マークアップ言語で記述されていることを特徴とする、請求項1又は2に記載の認証書類。

【請求項4】前記電子署名データが、前記認証内容データをハッシュ化し、認証者の秘密鍵で暗号化したデータであることを特徴とする、請求項1乃至3のいずれかに記載の認証書類。

【請求項5】前記バーコードが、2次元バーコードであることを特徴とする、請求項1乃至4のいずれかに記載の認証書類。

【請求項6】前記データが、直接バーコード化できない場合、テキストデータに変換してからバーコード化されていることを特徴とする、請求項1乃至4のいずれかに記載の認証書類。

【請求項7】前記電子証明書データが、認証機関によって認証された、認証者の公開鍵や署名アルゴリズムであることを特徴とする、請求項2に記載の認証書類。

【請求項8】認証者情報や認証者印影、及び、認証者の電子証明書データが予め印刷されていることを特徴とする認証用紙。

【請求項9】データベースから認証内容を記述した認証内容データを呼び出す手順と、

前記認証内容を記述したデータを暗号化して電子署名データを作成する手順と、

各データをバーコード化する手順と、

視覚により確認可能な認証内容、認証者情報及び認証者印影、前記認証内容を記述した認証内容データのバーコード、及び、該認証内容データを暗号化した電子署名データのバーコードを印刷する手順と、

を含むことを特徴とする認証書類の発行方法。

【請求項10】更に、認証機関による認証者の電子証明書データを呼び出す手順と、

該電子証明書データをバーコード化する手順と、

該バーコードを印刷する手順と、

を含むことを特徴とする、請求項9に記載の認証書類の発行方法。

【請求項11】更に、前記認証内容データをマークアップ言語化する手順を含むことを特徴とする、請求項9又は10に記載の認証書類の発行方法。

【請求項12】更に、直接バーコード化できないデータ

を、テキストデータに変換する手順を含むことを特徴とする、請求項9乃至11のいずれかに記載の認証書類の発行方法。

【請求項13】前記認証内容データをハッシュ化し、認証者の秘密鍵で暗号化することにより、前記電子署名データを作成することを特徴とする、請求項9乃至12のいずれかに記載の認証書類の発行方法。

【請求項14】データベースから認証内容を記述した認証内容データを呼び出す手段と、

前記認証内容を記述したデータを暗号化して電子署名データを作成する手段と、

各データをバーコード化する手段と、

視覚により確認可能な認証内容、認証者情報及び認証者印影、前記認証内容を記述した認証内容データのバーコード、及び、該認証内容データを暗号化した電子署名データのバーコードを印刷する手段と、

を含むことを特徴とする認証書類の発行装置。

【請求項15】データベースから認証内容を記述した認証内容データを呼び出す手段と、

前記認証内容を記述したデータを暗号化して電子署名データを作成する手段と、

認証機関による認証者の電子証明書データを呼び出す手段と、

各データをバーコード化する手段と、

視覚により確認可能な認証内容、認証者情報及び認証者印影、前記認証内容を記述した認証内容データのバーコード、該認証内容データを暗号化した電子署名データのバーコード、及び、前記電子証明書データのバーコードを印刷する手段と、

を含むことを特徴とする認証書類の発行装置。

【請求項16】視覚により確認可能な認証内容、認証者情報及び認証者印影、前記認証内容を記述した認証内容データのバーコード、及び、該認証内容データを暗号化した電子署名データのバーコードが共に印刷された認証書類から、バーコードを読み取る手順と、

読み取った電子署名データを復号化する手順と、

該復号化した電子署名データと前記認証内容データをハッシュ化したものを比較して、改ざんの有無と認証者の本人性を判定する手順と、

を含むことを特徴とする認証書類の検証方法。

【請求項17】更に、前記認証書類に印刷されている、認証機関による認証者の電子証明書データのバーコードを読み取る手順を含むことを特徴とする、請求項16に記載の認証書類の検証方法。

【請求項18】更に、事前に入手している、認証機関による認証者の電子証明書データを呼び出す手順を含むことを特徴とする、請求項16に記載の認証書類の検証方法。

【請求項19】前記電子証明書データに含まれる認証者の公開鍵を用いて、前記電子署名データを復号化するこ

【特許請求の範囲】

【請求項1】視覚により確認可能な認証内容、認証者情報及び認証者印影と、

前記認証内容を記述した認証内容データのバーコード、及び、該認証内容データを暗号化した電子署名データのバーコードと、

が共に記載されていることを特徴とする認証書類。

【請求項2】前記認証書類に、更に、認証機関による認証者の電子証明書データのバーコードが記載されていることを特徴とする、請求項1に記載の認証書類。

【請求項3】前記認証内容データが、マークアップ言語で記述されていることを特徴とする、請求項1又は2に記載の認証書類。

【請求項4】前記電子署名データが、前記認証内容データをハッシュ化し、認証者の秘密鍵で暗号化したデータであることを特徴とする、請求項1乃至3のいずれかに記載の認証書類。

【請求項5】前記バーコードが、2次元バーコードであることを特徴とする、請求項1乃至4のいずれかに記載の認証書類。

【請求項6】前記データが、直接バーコード化できない場合、テキストデータに変換してからバーコード化されていることを特徴とする、請求項1乃至4のいずれかに記載の認証書類。

【請求項7】前記電子証明書データが、認証機関によって認証された、認証者の公開鍵や署名アルゴリズムであることを特徴とする、請求項2に記載の認証書類。

【請求項8】認証者情報や認証者印影、及び、認証者の電子証明書データが予め印刷されていることを特徴とする認証用紙。

【請求項9】データベースから認証内容を記述した認証内容データを呼び出す手順と、

前記認証内容を記述したデータを暗号化して電子署名データを作成する手順と、

各データをバーコード化する手順と、

視覚により確認可能な認証内容、認証者情報及び認証者印影、前記認証内容を記述した認証内容データのバーコード、及び、該認証内容データを暗号化した電子署名データのバーコードを印刷する手順と、

を含むことを特徴とする認証書類の発行方法。

【請求項10】更に、認証機関による認証者の電子証明書データを呼び出す手順と、

該電子証明書データをバーコード化する手順と、

該バーコードを印刷する手順と、

を含むことを特徴とする、請求項9に記載の認証書類の発行方法。

【請求項11】更に、前記認証内容データをマークアップ言語化する手順を含むことを特徴とする、請求項9又は10に記載の認証書類の発行方法。

【請求項12】更に、直接バーコード化できないデータ

を、テキストデータに変換する手順を含むことを特徴とする、請求項9乃至11のいずれかに記載の認証書類の発行方法。

【請求項13】前記認証内容データをハッシュ化し、認証者の秘密鍵で暗号化することにより、前記電子署名データを作成することを特徴とする、請求項9乃至12のいずれかに記載の認証書類の発行方法。

【請求項14】データベースから認証内容を記述した認証内容データを呼び出す手段と、

前記認証内容を記述したデータを暗号化して電子署名データを作成する手段と、

各データをバーコード化する手段と、

視覚により確認可能な認証内容、認証者情報及び認証者印影、前記認証内容を記述した認証内容データのバーコード、及び、該認証内容データを暗号化した電子署名データのバーコードを印刷する手段と、

を含むことを特徴とする認証書類の発行装置。

【請求項15】データベースから認証内容を記述した認証内容データを呼び出す手段と、

前記認証内容を記述したデータを暗号化して電子署名データを作成する手段と、

認証機関による認証者の電子証明書データを呼び出す手段と、

各データをバーコード化する手段と、

視覚により確認可能な認証内容、認証者情報及び認証者印影、前記認証内容を記述した認証内容データのバーコード、該認証内容データを暗号化した電子署名データのバーコード、及び、前記電子証明書データのバーコードを印刷する手段と、

を含むことを特徴とする認証書類の発行装置。

【請求項16】視覚により確認可能な認証内容、認証者情報及び認証者印影、前記認証内容を記述した認証内容データのバーコード、及び、該認証内容データを暗号化した電子署名データのバーコードが共に印刷された認証書類から、バーコードを読み取る手順と、

読み取った電子署名データを復号化する手順と、

該復号化した電子署名データと前記認証内容データをハッシュ化したものを比較して、改ざんの有無と認証者の本人性を判定する手順と、

を含むことを特徴とする認証書類の検証方法。

【請求項17】更に、前記認証書類に印刷されている、認証機関による認証者の電子証明書データのバーコードを読み取る手順を含むことを特徴とする、請求項16に記載の認証書類の検証方法。

【請求項18】更に、事前に入手している、認証機関による認証者の電子証明書データを呼び出す手順を含むことを特徴とする、請求項16に記載の認証書類の検証方法。

【請求項19】前記電子証明書データに含まれる認証者の公開鍵を用いて、前記電子署名データを復号化するこ

の真贋の確認を行うものとして、特開2000-148742には、印章やサインイメージの近傍に、その管理番号及び使用番号をバーコード形式で付記すると共に、印字文書の中に、文書の管理番号及び保管機関のコードをバーコード形式で付記し、認証管理システム、及び、認証管理方法の実現のため電子文書を保管する電子文章データ保管システムと、個人や法人の印章やサイン等のイメージデータを認証データとして保管する認証データ保管システムで、相互に認証データの管理番号と文章管理番号を保管及び管理することが記載されている。

【0014】この方法によれば、印章やサインイメージの真贋の確認は容易となるが、文書の内容はバーコード化されていないので、文書内容の電子データ化に際しては、やはり前記のような問題点を生じる。

【0015】又、特表平9-512114には、ファクシミリでの文書送信において、元文書全体を画像スキャンし、圧縮・符号化し、バーコード化して認証することが記載されている。

【0016】しかしながら、この方法は、特殊機能を持つファクシミリ同士のやりとりでしか利用できない。又、本文書の画像スキャンしたラスタデータをそのままやりとりするため、何らかの方法でテキストデータ化しないと、本文の内容を2次利用できない等の問題点を有していた。

【0017】本発明は、前記従来の問題点を解消するべくなされたもので、紙ベースの認証システムと電子認証システムの両方で利用可能であり、電子データ化が容易で、且つ、改竄防止性能も高い認証書類を提供することを第1の課題とする。

【0018】本発明は、又、前記認証書類の作成に適した認証用紙を提供することを第2の課題とする。

【0019】本発明は、又、前記認証書類の発行方法及び装置を提供することを第3の課題とする。

【0020】本発明は、又、前記認証書類の検証方法及び装置を提供することを第4の課題とする。

【0021】

【課題を解決するための手段】本発明は、認証書類に、視覚により確認可能な認証内容、認証者情報及び認証者印影と、前記認証内容を記述した認証内容データのバーコード、及び、該認証内容データを暗号化した電子署名データのバーコードと、を共に記載することにより、前記第1の課題を解決したものである。

【0022】更に、前記認証書類に、認証機関による認証者の電子証明書データのバーコードも記載したものである。

【0023】又、前記認証内容データを、マークアップ言語で記述したものである。

【0024】又、前記電子署名データを、前記認証内容データをハッシュ化し、認証者の秘密鍵で暗号化したデータとしたものである。

【0025】又、前記バーコードを、2次元バーコードとしたものである。

【0026】又、前記データが、直接バーコード化できない場合、テキストデータに変換してからバーコード化したものである。

【0027】又、前記電子証明書データを、認証機関によって認証された、認証者の公開鍵や署名アルゴリズムとしたものである。

【0028】本発明は、又、認証用紙に、認証者情報や認証者印影、及び、認証者の電子証明書データを予め印刷することにより、前記第2の課題を解決したものである。

【0029】本発明は、又、データベースから認証内容を記述した認証内容データを呼び出す手順と、前記認証内容を記述したデータを暗号化して電子署名データを作成する手順と、各データをバーコード化する手順と、視覚により確認可能な認証内容、認証者情報及び認証者印影、前記認証内容を記述した認証内容データのバーコード、及び、該認証内容データを暗号化した電子署名データのバーコードを印刷する手順とにより、認証書類を発行するようにして、前記第3の課題を解決したものである。

【0030】更に、認証機関による認証者の電子証明書データを呼び出す手順と、該電子証明書データをバーコード化する手順と、該バーコードを印刷する手順と、を含むようにしたものである。

【0031】更に、前記認証内容データをマークアップ言語化する手順を含むようにしたものである。

【0032】更に、直接バーコード化できないデータを、テキストデータに変換する手順を含むようにしたものである。

【0033】又、前記認証内容データをハッシュ化し、認証者の秘密鍵で暗号化することにより、前記電子署名データを作成するようにしたものである。

【0034】本発明は、又、認証書類の発行装置を、データベースから認証内容を記述した認証内容データを呼び出す手段と、前記認証内容を記述したデータを暗号化して電子署名データを作成する手段と、各データをバーコード化する手段と、視覚により確認可能な認証内容、認証者情報及び認証者印影、前記認証内容を記述した認証内容データのバーコード、及び、該認証内容データを暗号化した電子署名データのバーコードを印刷する手段を用いて構成することにより、前記第3の課題を解決したものである。

【0035】本発明は、又、認証書類の発行装置を、データベースから認証内容を記述した認証内容データを呼び出す手段と、前記認証内容を記述したデータを暗号化して電子署名データを作成する手段と、認証機関による認証者の電子証明書データを呼び出す手段と、各データをバーコード化する手段と、視覚により確認可能な認証

内容、認証者情報及び認証者印影、前記認証内容を記述した認証内容データのバーコード、該認証内容データを暗号化した電子署名データのバーコード、及び、前記電子証明書データのバーコードを印刷する手段と、を用いて構成することにより、前記第3の課題を解決したものである。

【0036】本発明は、又、視覚により確認可能な認証内容、認証者情報及び認証者印影、前記認証内容を記述した認証内容データのバーコード、及び、該認証内容データを暗号化した電子署名データのバーコードが共に印刷された認証書類から、バーコードを読み取る手順と、読み取った電子署名データを復号化する手順と、該復号化した電子署名データと前記認証内容データをハッシュ化したものを比較して、改ざんの有無と認証者の本人性を判定する手順とにより、認証書類を検証するようにして、前記第4の課題を解決したものである。

【0037】更に、前記認証書類に印刷されている、認証機関による認証者の電子証明書データのバーコードを読み取る手順を含むようにしたものである。

【0038】又は、事前に入手している、認証機関による認証者の電子証明書データを呼び出す手順を含むようにしたものである。

【0039】又、前記電子証明書データに含まれる認証者の公開鍵を用いて、前記電子署名データを復号化するようにしたものである。

【0040】本発明は、又、認証書類の検証装置を、視覚により確認可能な認証内容、認証者情報及び認証者印影、前記認証内容を記述した認証内容データのバーコード、該認証内容データを暗号化した電子署名データのバーコード、及び、認証機関による認証者の電子証明書データのバーコードが共に印刷された認証書類から、バーコードを読み取る手段と、読み取った電子署名データを復号化する手段と、該復号化した電子署名データと前記認証内容データをハッシュ化したものを比較して、改ざんの有無を判定する手段を用いて構成することにより、前記第4の課題を解決したものである。

【0041】本発明は、又、認証書類の検証装置を、視覚により確認可能な認証内容、認証者情報及び認証者印影、前記認証内容を記述した認証内容データのバーコード、及び、該認証内容データを暗号化した電子署名データのバーコードが共に印刷された認証書類から、バーコードを読み取る手段と、事前に入手している、認証機関による認証者の電子証明書データを呼び出す手段と、読み取った電子署名データを復号化する手段と、該復号化した電子署名データと前記認証内容データをハッシュ化したものを比較して、改ざんの有無及び認証者の本人性を判定する手段とを用いて構成することにより、前記第4の課題を解決したものである。

【0042】

【発明の実施の形態】以下図面を参照して、本発明の実

施形態を詳細に説明する。

【0043】今、図1に示す如く、紙ベースの認証システムで運用している部門Aと、電子認証システムで運用している部門Bと、部門Aと部門Bを電子認証している、例えば最上位に位置するルート認証局あるいは信頼できる中間認証局である上位（管理）部門C（認証機関）を想定する。

【0044】前記部門Aには、例えば、認証内容のデータベースを含むパソコン10A及び認証書類発行用のプリンタ12Aが備えられている。この部門Aには、矢印Dに示す如く、上位部門Cから当該部門Aの秘密鍵データ20Aと、当該部門Aの公開鍵を含み、上位部門Cの電子署名がされている、部門Aの電子証明書データ22Aと、上位部門Cの公開鍵を含む、部門Cの電子証明書データ（図示省略）が配布されているとする。

【0045】又、前記部門Bには、例えば、部門Aと同様のパソコン10B及びプリンタ12Bと、バーコードリーダ14とが備えられている。この部門Bには、矢印Eに示す如く、上位部門Cから、当該部門Bの秘密鍵データ20Bと、当該部門Bの公開鍵を含み、上位部門Cの電子署名がされている、部門Bの電子証明書データ22Bと、上位部門Cの公開鍵を含む、部門Cの電子証明書データ（図示省略）を配布されているとする。

【0046】まず、矢印Fに示す如く、紙ベースの認証システムの部門Aで発行した認証書類30Aを、電子認証システムの部門Bで事務処理する場合について説明する。

【0047】部門Aで認証書類30Aを発行する手順を図2に示す。

【0048】部門Aでは、認証書類の発行要求者の要望に応じて、ステップ100で認証内容32Aをデータベースから呼び出し、呼び出したデータを、必要に応じてXML等のマークアップ言語で記述すると共に、バーコードの仕様上、直接バーコード化できないバイナリデータは、例えばBase64でテキストデータに変換して、認証内容データとする。

【0049】次いでステップ102で、該認証内容データを、例えばハッシュ化してメッセージダイジェストを作成し、部門Aの秘密鍵データ20Aで暗号化して電子署名データを作成する。

【0050】次いでステップ104で、必要に応じて、部門Aの上位部門Cによる電子証明書データ22Aを呼び出す。なお、部門Aと部門Bが頻繁に認証書類をやり取りする際には、事前に部門Aと部門Bとが、上位部門Cによって認証された部門Aと部門Bの電子証明書データを交換しておくことによって、認証書類の電子証明書データを省略することもできる。この場合には、ステップ104は不要である。

【0051】次いでステップ106、108、110で、前出ステップ100、102、104で作成された

データを、それぞれ、例えば2次元バーコード化する。なお、バーコード化する順番は任意であり、特に認証書類の電子証明書データを省略した場合には、当然ステップ110も不要である。

【0052】次いでステップ112に進み、図1に符号30Aで示す如く、従来の紙の認証書類に記載されていた認証内容（ここでは文章）32A、部門Aの名称34A、部門Aの印影36Aに加えて、認証内容32Aのバーコード33A、ステップ102で作成された電子署名データのバーコード38A、及び、ステップ104で作成された電子証明書データのバーコード40Aを印刷して、紙の認証書類30Aとする。

【0053】次に、前記のようにして作成された紙の認証書類30Aは、図3に示すような手順に従って、部門Bにより検証される。

【0054】即ち、部門Bでは、まずステップ200、202、204で、紙の認証書類30Aから、例えばバーコードリーダ14（スキャナでも良い）を用いて、バーコード33A（認証内容）、バーコード38A（電子署名データ）、バーコード40A（電子証明書）を読み取る。この際、Base64でテキストデータに変換されていたバイナリデータは、Base64で逆変換してバイナリデータに戻す。又、電子証明書データのバーコードが省略されている場合には、ステップ204で、事前に入手している電子証明書データを呼び出す。

【0055】次いでステップ206で、部門Cの電子証明書データを基に、例えばバーコード40Aに記述された部門Aの電子証明書データ22Aが上位部門Cで認証されていることを確認したら、該電子証明書データ22Aに含まれる部門Aの公開鍵データを取り出す。

【0056】次いでステップ208に進み、ステップ206で取り出した公開鍵を用いて、ステップ202で読み取った電子署名データを復号化し、メッセージダイジェストiを作成する。

【0057】次いでステップ210に進み、ステップ200で読み取った認証内容データをハッシュ化して、メッセージダイジェストiiを作成する。

【0058】次いでステップ212に進み、メッセージダイジェストiとiiを比較し、一致する場合には、ステップ214で、認証内容の本人認証と非改ざんを確認する。

【0059】一方、メッセージダイジェストiとiiが不一致の場合には、ステップ216に進み、認証内容の本人認証及び非改ざんを承認しない。

【0060】このようにして、認証書類の内容の電子化、認証内容の非改ざんの証明、及び認証書類の部門Aの本人証明を実現することができ、内容を確認した後、直ちに電子データを電子認証システムで扱うことが可能となる。

【0061】一方、電子認証システムの部門Bで認証し

た書類を、図1の矢印Gに示す如く、紙ベースの認証の部門Aで事務処理する場合には、部門Aの場合と同様に、部門Bでも、従来の認証内容32B、部門Bの名称34B、部門Bの印影36Bに加えて、認証内容をマークアップ言語で記述した認証内容データ、これをハッシュ化して部門Bの秘密鍵で暗号化した電子署名データ、上位部門Cによって証明されている部門Bの電子証明書データを、それぞれ例えば2次元バーコード33B、38B、40B化し、紙の認証書類30Bとして印刷する。この際、バイナリデータであって、バーコードの仕様上、直接バーコード化できない場合には、例えばBase64でテキストデータに変換してからバーコード化する。

【0062】この認証書類30Bを、部門Aでは、紙ベースであるので、従来と同様に、認証内容32B、部門名称34B、部門印36Bにより目視で内容を確認する。なお、何らかの不具合等で、部門Aから部門Bに認証書類を返送する必要がある場合には、部門Bでは、バーコードリーダ14でバーコードを読み取って、再度内容を取り込むことが可能である。

【0063】本実施形態においては、バーコードとして、2次元バーコードを用いているので、少ない面積で、多くの情報を記述できる。なお、バーコードの種類は、これに限定されない。

【0064】又、本実施形態においては、バーコードの仕様上、直接バーコード化できない場合には、Base64でテキストデータに変換してからバーコード化するようにしているので、バイナリデータであっても、バーコード化可能である。なお、バイナリデータをテキストデータに変換する方式はBase64に限定されず、例えばUNIX（登録商標）標準のuuencodeや、Macintoshで用いられているBinHexといった方式を用いることも可能である。

【0065】更に、本実施形態においては、マークアップ言語XMLのデータにしてからバーコード化しているので、項目と内容が明瞭となり、認証内容の2次利用が容易である。なお、マークアップ言語の種類はXMLに限定されず、HTML、TEX、SGML等を用いることも可能である。又、マークアップ言語化を省略することも可能である。

【0066】なお、前記実施形態においては、全ての情報をプリンタで印刷するようにしていたが、例えば図4に示す如く、認証者情報34や認証者印影36、及び、認証者の電子証明書データのバーコード40等の固定されたデータが予め印刷されている認証用紙50を用いて、印刷の負荷を軽減することも可能である。

【0067】本発明の適用対象は、地方自治体における証明書発行や登録処理に限定されず、一般の領収書発行や、会計処理等にも同様に用いることができることは明らかである。

【0068】

【発明の効果】本発明によれば、認証書類の内容の電子化、認証書類の非改ざんの証明、認証書類の認証者の本人証明を実現でき、紙ベースの認証システムと電子認証システムのどちらでも利用可能であるという優れた効果を有する。

【図面の簡単な説明】

【図1】本発明に係る認証書類の発行方法及び検証方法を実施するシステムの例の全体構成を示すブロック線図

【図2】本発明の実施形態における認証書類の発行手順を示す流れ図

【図3】同じく認証書類の検証手順を示す流れ図

【図4】同じく認証用紙の例を示す正面図

【符号の説明】

A、B…部門

C…上位部門（認証機関）

10A、10B…パソコン

12A、12B…プリンタ

14…バーコードリーダー

20A、20B…秘密鍵データ

22A、22B…電子証明書データ

30A、30B…認証書類

32A、32B…認証内容

34、34A、34B…部門名称

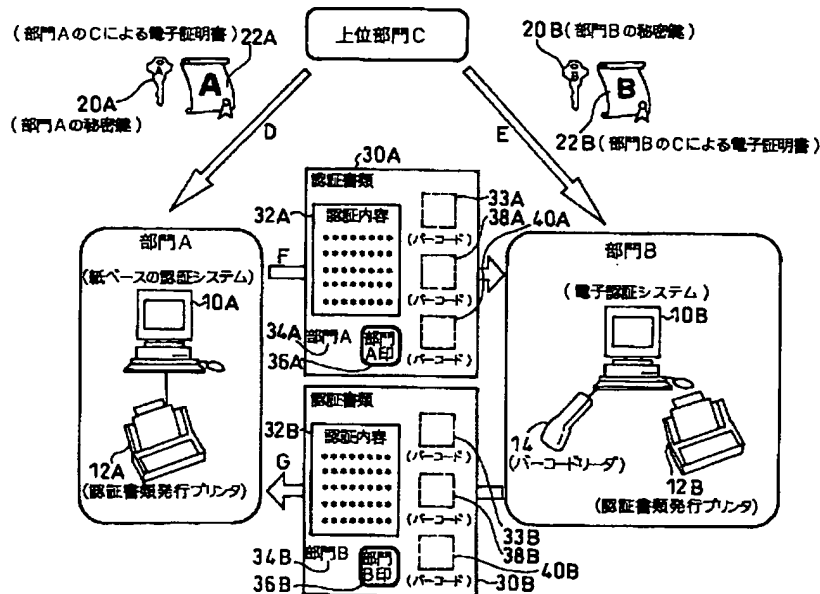
36、36A、36B…部門印

33A、33B、38A、38B、40、40A、40

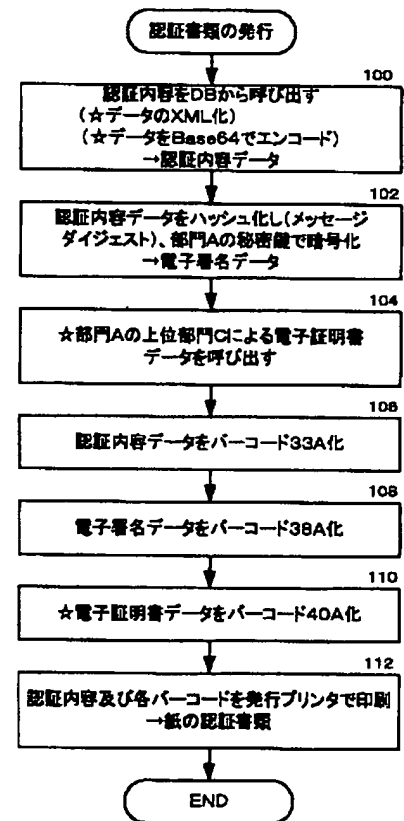
B…バーコード

50…認証用紙

【図1】

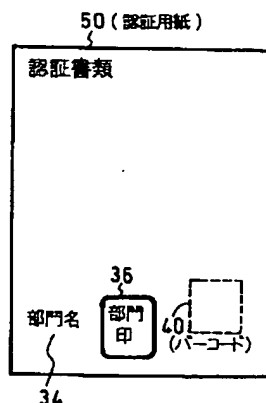


【図2】

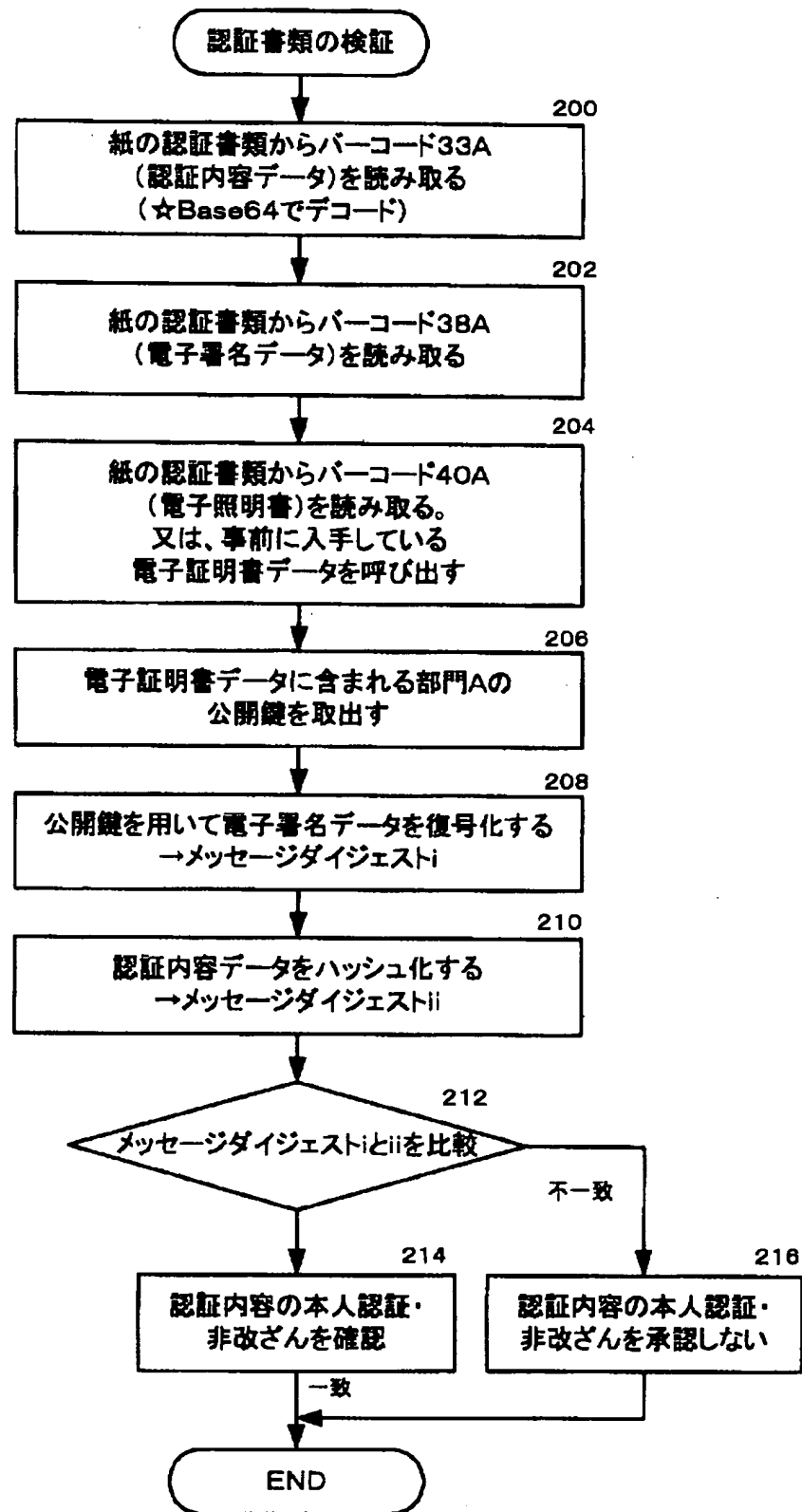


★はオプション

【図4】



【図3】



☆はオプション

フロントページの続き

(51)Int.Cl.⁷

識別記号

F I

テレポート (参考)

G 0 6 K 19/06

G 0 7 D 7/20

G 0 7 D 7/20

G 0 6 K 19/00

A